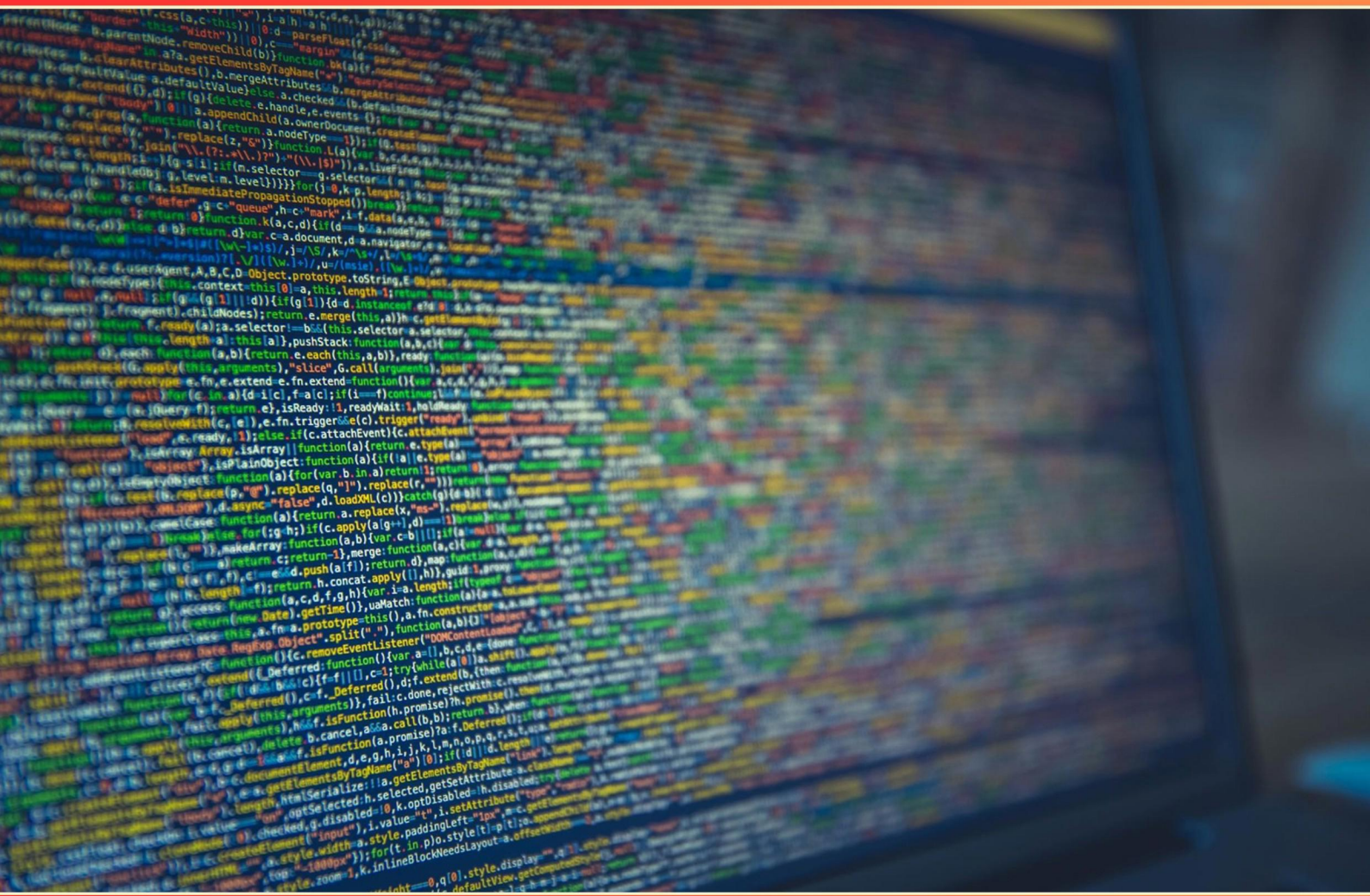
CERTIFIED ETHICAL HACKER VERSION 11 (CEHV11) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cehv11.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. **Which DNS poisoning scenario involves infecting John's machine with a Trojan to change his DNS IP address to the attacker's?**

   A. Internet DNS poisoning

   B. DNS cache poisoning

   C. Proxy server DNS poisoning

   D. Intranet DNS spoofing attack

2. **What term describes a collection of computers and peripherals connected as one entity?**

   A. Network

   B. Subnet

   C. Virus

   D. Domain

3. **Which keylogger type attaches to the PS/2 or USB interface and does not require software to function?**

   A. PS/2 and USB Keylogger

   B. Bluetooth Keylogger

   C. Acoustic/CAM Keylogger

   D. Wi-Fi Keylogger

4. **Which formula represents the risk equation?**

   A. Risks = Threats x Vulnerabilities

   B. Risks = Threats / Vulnerabilities

   C. Risk = Threat x Vulnerabilities

   D. Risks = Threats - Vulnerabilities

5. **Which Sublist3r option is used to write results to a file?**

   A. -d DOMAIN

   B. -t THREADS

   C. -e ENGINES

   D. -o OUTPUT

SAMPLE

6. Which term best describes a web service designed using REST principles and HTTP methods, providing access to resources via standard verbs such as GET, POST, PUT, and DELETE?

A. REST

B. RESTful API

C. Stateless

D. Cacheable

7. What is the act of altering logs to evade legal action?

A. Auditpol

B. Manipulating Logs

C. Clearing Logs

D. Covering Tracks on the Network

8. The DNS record that points to the host's IP address and is commonly used for IPv4 is:

A. MX

B. SOA

C. A

D. NS

9. An XML parser misconfiguration allows an attacker to abuse external entities and access restricted resources. This attack is called:

A. XML External Entity Attack

B. Broken Authentication

C. Timeout Exploitation

D. Insecure Direct Object References

10. Which Google search pattern would locate pages that have a login page title and a specific utility name in the text?

A. inurl:login intext:Phone

B. intitle:Login Page

C. intitle:Login Page intext:Phone

D. intitle:"Login Page" intext:"Phone Adapter Configuration Utility"

SAMPLE

Answers

SAMPLE

1. A
2. D
3. A
4. A
5. D
6. B
7. B
8. C
9. A
10. D

SAMPLE

Explanations

SAMPLE

1. Which DNS poisoning scenario involves infecting John's machine with a Trojan to change his DNS IP address to the attacker's?

A. Internet DNS poisoning

B. DNS cache poisoning

C. Proxy server DNS poisoning

D. Intranet DNS spoofing attack

This scenario tests client-side DNS manipulation through malware. When a Trojan infects John's machine and changes the DNS IP address that the host uses, all DNS lookups from that machine are sent to an attacker-controlled DNS server. The attacker can then respond with false IPs, redirecting John's traffic to malicious sites or enabling man-in-the-middle activity. This kind of DNS redirection happens because the compromised host itself is directing queries to a rogue DNS server, not because the DNS resolver's cache was poisoned or because a proxy or internal network service was tampered with. It's different from DNS cache poisoning, which targets a DNS server's cached records and can mislead many users who rely on that resolver, rather than altering an individual host's settings. It's also distinct from proxy server DNS poisoning, which would involve compromising a proxy to mislead clients behind it, and from intranet spoofing, which typically targets internal network services rather than the end-user host's DNS configuration.

2. What term describes a collection of computers and peripherals connected as one entity?

A. Network

B. Subnet

C. Virus

D. Domain

A domain is a centralized administrative boundary that groups computers and peripherals under a single management framework. It defines a shared directory service and a common set of policies, so all devices and users within the domain can be authenticated, authorized, and managed from centralized controllers. This makes the entire collection behave as one entity for tasks like logging in, deploying software, and enforcing security settings. While a network describes how devices are physically or logically connected, a domain emphasizes unified administration and security across those devices. Subnets are just subdivisions of a network for IP addressing and routing, and a virus is malicious software, not a structural concept for organizing devices.

3. Which keylogger type attaches to the PS/2 or USB interface and does not require software to function?

A. PS/2 and USB Keylogger

B. Bluetooth Keylogger

C. Acoustic/CAM Keylogger

D. Wi-Fi Keylogger

Hardware keyloggers sit between the keyboard and the computer, capturing keystrokes at the hardware interface. When a device plugs into PS/2 or USB, it logs what the user types without needing any software on the target machine to run. This makes it independent of the host OS and applications, so it can function even if the computer is offline or has strict security controls. The other options rely on wireless transmission (Bluetooth or Wi Fi) or environmental capture (acoustic/cam), which require additional components, software, or configurations to exfiltrate the data. Thus, the inline PS/2/USB hardware keylogger is the best fit.

SAMPLE

4. Which formula represents the risk equation?

A. Risks = Threats x Vulnerabilities

B. Risks = Threats / Vulnerabilities

C. Risk = Threat x Vulnerabilities

D. Risks = Threats - Vulnerabilities

In information security, risk is understood as something that rises when there are both a threat and a vulnerability present, and it grows as either factor increases. Modeling risk as a product of threats and vulnerabilities captures this idea: the more threats you face and the more vulnerabilities you have, the higher the overall risk. Multiplication also makes sense because if either factor is zero, the risk drops to zero—no threats or no vulnerabilities means no risk. The given formula uses this multiplicative relationship consistently, matching the common way risk is represented in many practice contexts. It's worth noting that some models expand the equation to include impact as a third factor (risk = threat × vulnerability × impact), but for this item, the two-factor, multiplicative form is the best fit. The other forms—dividing, subtracting, or mixing singular/plural forms—do not reflect how risk scales when both threats and vulnerabilities are present.

5. Which Sublist3r option is used to write results to a file?

A. -d DOMAIN

B. -t THREADS

C. -e ENGINES

D. -o OUTPUT

The ability to save results to a file in Sublist3r is provided by the -o option, which takes a file path after it (for example, -o output.txt). This flag directs Sublist3r to write the discovered subdomains to that file instead of printing them to the screen. The other flags configure what to search or how the search runs: -d sets the domain to target, -t controls the number of threads used, and -e selects which engines to use. These don't specify a file for output, so they don't save results by themselves. So the -o OUTPUT option is the correct one for writing results to a file.

6. Which term best describes a web service designed using REST principles and HTTP methods, providing access to resources via standard verbs such as GET, POST, PUT, and DELETE?

A. REST

B. RESTful API

C. Stateless

D. Cacheable

Using REST principles to build a web service means you expose resources via URIs and interact with them using standard HTTP methods like GET, POST, PUT, and DELETE to read, create, update, or delete those resources. The term that best describes this kind of service is a RESTful API. REST describes the architectural style and constraints, while a RESTful API is the concrete implementation that follows those rules and provides endpoints you can call with HTTP methods. Why this fits: the emphasis is on how the service is designed and accessed—through resources and standard verbs—so calling it a RESTful API communicates both adherence to REST and the fact that it's an actual, callable service rather than a theoretical description. Reasoning about the other terms: REST by itself refers to the architectural style, not the specific service implementation. Stateless and Cacheable are constraints within REST that describe how interactions should behave rather than naming the service itself. They are important characteristics, but they don't denote the type of web service as clearly as RESTful API does.

SAMPLE

7. What is the act of altering logs to evade legal action?

A. Auditpol

B. Manipulating Logs

C. Clearing Logs

D. Covering Tracks on the Network

Tampering with log data is about changing entries to mislead investigators and avoid accountability. When someone edits, backdates, or inserts false events into logs, they are manipulating logs to cover their tracks and evade legal action. This term directly captures the act of altering the record itself, which is why it's the best fit for the scenario. In practice, defenders emphasize log integrity through tamper-evident storage and integrity checks to prevent and detect such manipulation. Configuring auditing policies isn't about altering logs, clearing logs means deleting them, and covering tracks on the network is a broader tactic that includes more than just changing log entries.

8. The DNS record that points to the host's IP address and is commonly used for IPv4 is:

A. MX

B. SOA

C. A

D. NS

In DNS, translating a human-friendly hostname into a numeric address that devices can connect to is essential for routing traffic. The record that binds a domain name to its IPv4 address is the A record. It associates the hostname with a 32-bit IPv4 address, enabling clients to reach the host over IPv4. For IPv6, the equivalent is the AAAA record. Other common records have different roles: MX directs mail to a mail server, NS designates the authoritative name servers for a domain, and SOA holds authority and caching information for the zone. So, for mapping to an IPv4 address, the A record is the correct choice.

9. An XML parser misconfiguration allows an attacker to abuse external entities and access restricted resources. This attack is called:

A. XML External Entity Attack

B. Broken Authentication

C. Timeout Exploitation

D. Insecure Direct Object References

This question tests XXE, XML External Entity attack. It happens when an XML parser is misconfigured to process external entity declarations, allowing an attacker to cause the parser to fetch or reveal restricted resources. By crafting XML that defines entities pointing to local files (like file:///etc/passwd) or internal network resources, the attacker can cause the parser to disclose sensitive data or reach resources that should be inaccessible. This exposure occurs because the parser is trusted to resolve those external references, so it ends up reading or relaying those resources to the attacker. Other concepts described in security literature involve different failure modes: broken authentication deals with weaknesses in verifying identities; insecure direct object references involve exposing internal object identifiers in inputs like URLs; and timeouts or related exploitation methods target performance or reliability, not the specific mechanism of an XML parser evaluating external entities.

SAMPLE

10. Which Google search pattern would locate pages that have a login page title and a specific utility name in the text?

A. inurl:login intext:Phone

B. intitle:Login Page

C. intitle:Login Page intext:Phone

D. intitle:"Login Page" intext:"Phone Adapter Configuration Utility"

The concept being tested is using Google search operators to constrain both the page title and the visible text, so you find a login page that also mentions a specific utility in its content. The best pattern is intitle:"Login Page" intext:"Phone Adapter Configuration Utility". The quotes lock in exact phrases, ensuring the page title contains the words Login Page and the body text contains the exact phrase Phone Adapter Configuration Utility. This precision is why it's the strongest match for a login page that also names that utility in the text. Other patterns either don't require the title, or don't lock the exact utility name in the text, which can return pages that aren't truly about that specific login page or miss pages that do mention the exact utility name.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://cehv11.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE